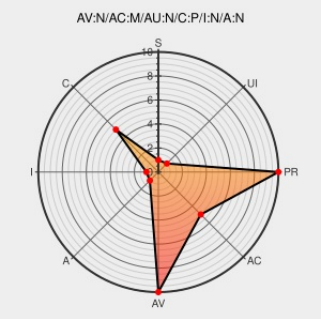
# CVE-2013-1824

Published on: 09/15/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:41:00 AM UTC

## CVE-2013-1824

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Mac Os X from Apple contain the following vulnerability:

The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.

CVE-2013-1824 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| 208.43.231.11 Git - php-src.git/commit | web.archive.org text/xml Inactive Link Not Archived | MISC git.php.net/?p=php-src.git%3Ba=commit%3Bh=188c196d4da60bdde9190d2fc532650d17f7af2d |
| Bug 918187 – CVE-2013-1643 php: Ability to read arbitrary files due use of external entities while parsing SOAP WSDL files | Patch bugzilla.redhat.com text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=918187 |
| CVE-2013-1824 in Ubuntu | people.canonical.com text/html | CONFIRM people.canonical.com/~ubuntu-security/cve/2013/CVE-2013-1824.html |
| 208.43.231.11 Git - php-src.git/commit | Patch web.archive.org text/xml | MISC git.php.net/?p=php-src.git%3Ba=commit%3Bh=afe98b7829d50806559acac9b530acb8283c3bf4 |

| | | |
|---|---|---|
| | Inactive Link Not Archived | |
| APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004 | lists.apple.com text/html | APPLE APPLE-SA-2013-09-12-1 |
| About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004 | support.apple.com text/html | CONFIRM support.apple.com/kb/HT5880 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Apple | Mac Os X | All | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.0 | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.1 | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.2 | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.0 | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.1 | All | All | All |
| Operating System | Apple | Mac Os X | 10.8.2 | All | All | All |
| Operating System | Apple | Mac Os X | All | All | All | All |
| Application | Php | Php | All | All | All | All |
| Application | Php | Php | 5.3.0 | All | All | All |
| Application | Php | Php | 5.3.1 | All | All | All |
| Application | Php | Php | 5.3.10 | All | All | All |
| Application | Php | Php | 5.3.11 | All | All | All |
| Application | Php | Php | 5.3.12 | All | All | All |
| Application | Php | Php | 5.3.13 | All | All | All |
| Application | Php | Php | 5.3.14 | All | All | All |
| Application | Php | Php | 5.3.15 | All | All | All |
| Application | Php | Php | 5.3.16 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Php | Php | 5.3.17 | All | All | All |
| Application | Php | Php | 5.3.18 | All | All | All |
| Application | Php | Php | 5.3.19 | All | All | All |
| Application | Php | Php | 5.3.2 | All | All | All |
| Application | Php | Php | 5.3.20 | All | All | All |
| Application | Php | Php | 5.3.3 | All | All | All |
| Application | Php | Php | 5.3.4 | All | All | All |
| Application | Php | Php | 5.3.5 | All | All | All |
| Application | Php | Php | 5.3.6 | All | All | All |
| Application | Php | Php | 5.3.7 | All | All | All |
| Application | Php | Php | 5.3.8 | All | All | All |
| Application | Php | Php | 5.3.9 | All | All | All |
| Application | Php | Php | 5.4.0 | All | All | All |
| Application | Php | Php | 5.4.1 | All | All | All |
| Application | Php | Php | 5.4.10 | All | All | All |
| Application | Php | Php | 5.4.11 | All | All | All |
| Application | Php | Php | 5.4.2 | All | All | All |
| Application | Php | Php | 5.4.3 | All | All | All |
| Application | Php | Php | 5.4.4 | All | All | All |
| Application | Php | Php | 5.4.5 | All | All | All |
| Application | Php | Php | 5.4.6 | All | All | All |
| Application | Php | Php | 5.4.7 | All | All | All |
| Application | Php | Php | 5.4.8 | All | All | All |
| Application | Php | Php | 5.4.9 | All | All | All |
| Application | Php | Php | 5.3.0 | All | All | All |
| Application | Php | Php | 5.3.1 | All | All | All |
| Application | Php | Php | 5.3.10 | All | All | All |
| Application | Php | Php | 5.3.11 | All | All | All |
| Application | Php | Php | 5.3.12 | All | All | All |
| Application | Php | Php | 5.3.13 | All | All | All |
| Application | Php | Php | 5.3.14 | All | All | All |
| Application | Php | Php | 5.3.15 | All | All | All |
| Application | Php | Php | 5.3.16 | All | All | All |
| Application | Php | Php | 5.3.17 | All | All | All |
| Application | Php | Php | 5.3.18 | All | All | All |
| Application | Php | Php | 5.3.19 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Php | Php | 5.3.2 | All | All | All |
| Application | Php | Php | 5.3.20 | All | All | All |
| Application | Php | Php | 5.3.3 | All | All | All |
| Application | Php | Php | 5.3.4 | All | All | All |
| Application | Php | Php | 5.3.5 | All | All | All |
| Application | Php | Php | 5.3.6 | All | All | All |
| Application | Php | Php | 5.3.7 | All | All | All |
| Application | Php | Php | 5.3.8 | All | All | All |
| Application | Php | Php | 5.3.9 | All | All | All |
| Application | Php | Php | 5.4.0 | All | All | All |
| Application | Php | Php | 5.4.1 | All | All | All |
| Application | Php | Php | 5.4.10 | All | All | All |
| Application | Php | Php | 5.4.11 | All | All | All |
| Application | Php | Php | 5.4.2 | All | All | All |
| Application | Php | Php | 5.4.3 | All | All | All |
| Application | Php | Php | 5.4.4 | All | All | All |
| Application | Php | Php | 5.4.5 | All | All | All |
| Application | Php | Php | 5.4.6 | All | All | All |
| Application | Php | Php | 5.4.7 | All | All | All |
| Application | Php | Php | 5.4.8 | All | All | All |
| Application | Php | Php | 5.4.9 | All | All | All |
| Application | Php | Php | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 5 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 5 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | All | All |

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.15:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.16:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.4.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→